



Технология и природа

Убить Дракона

*Все беды причиняют вред,
Конечно, лучше жить без бед,
Но не всегда, а иногда
Бывает польза от вреда.*

*Все беды отрицать нельзя:
В них познаются все друзья!
А в дни сплошных удач и благ
Не знаешь сам, кто друг, кто враг.*

Николай ГЛАЗКОВ

Недавно произошло малозаметное, но важное событие — у антивирусной программы Д. Н. Лозинского «AIDSTEST» появилась цена. И тронула больше всего не объявленная сумма (хороший труд должен хорошо оплачиваться), и не предприимчивость Дмитрия Николаевича (хотя всегда немного грустно, когда благие начинания кончаются подобным образом)... Дело в том, что переход гранда отечественной компьютерной вирусологии от коммунистических отношений к рыночным ознаменовал конец короткого, но очень бурного этапа развития всеобщей компьютеризации. Этот период — реальное, хотя, быть может, и несколько экстравагантное воплощение в жизнь мечты о всеобщем коммунистическом братстве, когда брат бескорыстно помогал брату (в основном чужими программами, чаще всего взятыми без спроса из-за рубежа). Борьба с компьютерными вирусами в надежде быстрого их искоренения как вида программ в то

время была заботой всего общества. Сейчас, когда свершился переход от всенародной борьбы с вирусами к текущей повседневной работе, пришло время проанализировать пройденный этап.

НАЧАЛА И КОНЦЫ

Образ вируса, как ничто другое в программировании, вдохновляет народное творчество. Кроме полнокровного фольклора (сказки, легенды, тосты) сложился и обширный слой околокомпьютерной литературы, посвященной вирусам. Их необычные свойства — мистические (по слухам) способности, неофициальный характер распространения (близость к народу), относительная простота изготовления — породили богатый спектр отношений: от официальных проклятий до всенародной любви, от страха у новичка до последней надежды у обиженного. В потоке публикаций, как в зеркале, отразились сложность и противоречивость отношения к вирусам. Но какого бы автора мы ни взяли, будь то прагматичный Лозинский или грозно назидательный Безруков, они не дают удовлетворительного ответа на принципиальные вопросы, касающиеся сущности и перспектив развития компьютерных вирусов.

Появление вирусов предсказал и обосновал еще Н. Виннер, а спровоцировал — размах компьютеризации. У каждого вируса есть конкретные родители (Иванов, Петров, Моррисон), и если бы этим программистам привили в детстве чуть больше любви к ближнему, то не пришлось бы теперь изобретать хитроумные способы антивирусной защиты.

Может сложиться впечатление, что достаточно нескольких удачных педагогических приемов при поддержке строгих уголовных законов, и с вирусами (не сразу, но в принципе) будет покончено. Однако, если взглянуть на этот вопрос шире, то к радужной картине (солнце, пальмы, золотой песок) придется добавить и крокодилов.

НИША ДЛЯ ПАРАЗИТА

Каковы общие закономерности паразитизма? Что роднит бактерию, мафиози и отрывок кода для ЭВМ?

Взгляните, как передаются паразиты при рукопожатии. Рукой мы управляем через несколько уровней-посредников: клеточный, нервный, мышечный, кожный. Каждый следующий уровень управления, выполняя приказы предыдущего, обладает некоторой свободой действий. Бывает так: хотел пожать руку, а дал по физиономии, но это скорее исключение. Обычно отклонения, вызван-

ные «творчеством» уровней-посредников, незначительны. Нервно-мышечный уровень может вызвать дрожание руки, неловкое пожатие, а кожный — способствовать передаче микроорганизмов. Определенная самостоятельность уровней и дает паразитам шанс на существование. Так и в государстве преступность процветает благодаря незамысловатой схеме: до Бога высоко, до царя далеко. Многочисленные промежуточные эшелоны власти управляют обществом в целом, но контролировать действия каждого члена не могут.

Вот так же через уровни-посредники обычный пользователь управляет ЭВМ. Когда вы решаете поиграть в «Tetris», то сначала передаете управление операционной системе, которая запускает рабочий файл, ни мало не интересуясь, чем он будет заниматься и сидит ли в нем вирус.

Проконтролировать работу программы, обнаружить спрятанных в ней паразитов операционная система пока не в состоянии. Значит, и здесь паразиты могут благополучно обитать, лишь бы имелись в системе по крайней мере два соподчиненных уровня управления. Эти уровни важны не сами по себе. Они обеспечивают многовариантность действий младшего уровня по команде старшего. Чем больше такое несоответствие, тем шире «экологическая» ниша для паразитов. Если система деградирует и ее управление разваливается или, наоборот, слишком торопится в развитии, громоздя уровни управления один на другой, то естественные при этом пустоты в управлении становятся дополнительными экологическими нишами для новых систем-паразитов.

Не подумайте, будто самоорганизация обязательно начинается с молекулярного уровня. Если появляется возможность существовать за чужой счет, желающие всегда найдутся, и необязательно это будут микробы.

РАЗБОЙНИКИ У ПРЕСТОЛА

Роль паразитов в природе и обществе неоднозначна и противоречива. В биологических системах на уровне отдельных особей паразит, как правило, наносит вред организму хозяина. На уровне популяции гибель части особей оказывается полезной. Действуя по принципу отрицательной обратной связи, паразит регулирует численность популяции, повышая при этом устойчивость системы паразит — хозяин.

В обществе та же картина. В послеоктябрьский период отечественные предприниматели (с официальной точки зрения) — паразиты, пьющие кровь трудового народа и

мешающие идти к светлому будущему. Мировое сообщество имеет несколько иной взгляд на бизнес.

Понятно, что, с точки зрения хозяина, паразит он и есть паразит: отбирает с трудом добытые ресурсы, мешает развитию. Однако в сообществе роль паразитов иная: если его члены прошли «проверку паразитами», то совокупность более устойчива. Это похоже на дом, выстроенный из отборных кирпичей: хотя строили и дольше, чем из первых попавшихся, зато получилось надежнее, долговечнее.

Для членов сообщества паразитизм тоже не всегда вреден. Бывает и взаимовыгодное партнерство, когда взросший паразит может стать если не кормильцем, то помощником. Да и в государстве бывшие разбойники иногда становятся опорой престола.

ОТКУДА И КУДА

Как это ни покажется странным, главная причина возникновения компьютерных вирусов — отсутствие взаимопонимания между человеком и машиной. Язык ЭВМ (машинные коды или ассемблер) оказался настолько неудобен для человека, что пришлось для нормального управления создать несколько промежуточных уровней — алгоритмические языки (Фортран, Паскаль...), операционные системы, оболочки (Norton Commander, XTree Gold...). Конечно, чудак-инженеры не специально сделали машинный язык таким тарабарским. Когда выяснилось, что двигающаяся лента с дырочками (машина Тьюринга — математический прообраз ЭВМ) может что-то считать, никто не думал о будущих трудностях общения человека и машины.

В современных персоналках воображаемая лента достигает сотен километров в длину и движется с бешеной скоростью. Понятно, что человек не может управлять машиной без посредников, а значит, необходимое условие для существования паразитов соблюдено.

В процессе развития машинно-человеческого общения появлялись все новые и новые промежуточные уровни, и каждый из них образовывал удобную нишу для своих паразитов. И все же наиболее благоприятные условия для вирусов предоставил самый нижний уровень — машинный код, на котором и написано подавляющее большинство паразитирующих программ. Минимальная длина программы-вируса — 100—1000 байт на языке ассемблера, а большинство прикладных программ на два-три порядка длиннее, и паразиту несложно затеряться в ее дебрях.

Авторы вирусов выполняют лишь повивальные (как сказал бы классик) функции, то есть помогают вирусу появиться на свет, окрашивая в меру своих способностей этот процесс в мрачные тона.

Разработка новых технологий общения между человеком и ЭВМ (экспертные системы, искусственный интеллект) вселяет надежду, что скоро появится язык более высокого уровня, близкий к человеческому, который вытеснит нынешние «процедурные» языки. Поэтому через несколько десятилетий компьютерная вирусология отступит на второй план. Достаточно будет сформулировать задачу на обычном (человеческом) языке, и ЭВМ сама создаст максимально эффективный алгоритм.

Однако свято место пусто не бывает — скоро образуется ниша и для электронно-алгоритмических паразитов, ведь рано или поздно машины станут обмениваться не только информацией, но и деталями, «железками».

Вот тут-то их и подстережет извечный спутник развития — паразит. И появятся машинные вирусы иных, более сложных уровней.

ВРАГ ИЛИ ДРУГ?

Первое, что бросается в глаза при чтении работ отцов отечественной вирусологии, — это возмущение и негодование по поводу вирусов. Образ вируса-врага очень похож на «страшных цыган» из пьесы Е. Шварца «Дракон». Их роднит официально-мифологическое происхождение и доверчивое народное осмысление. Убить Дракона по Шварцу, это всего лишь понять, что бывает не только так, как тебе втолковывали с детства. При этом носители добра и зла в твоём сознании могут поменяться местами.

Возможно, компьютерные вирусы не доживут до благодарности и всеобщего признания их прогрессивной роли (как в биологии или экономике), но они уже сейчас стали, с одной стороны, полигоном для испытания новых методов, а с другой, указателями недостатков системы человек+ЭВМ. Но дело даже не в том, что и компьютерные вирусы могут принести какую-то пользу. Понимая природу паразитизма, становится очевидным, что бессмысленно рассматривать вирусы с позиций добра и зла вообще, а следовательно, столь же бессмысленно огульно шельмовать авторов, вольно или невольно запустивших паразитов гулять по свету. Но новые технологии общения — дело будущего, а эффективные методы защиты от вирусов нужны сегодня.

Подобный сценарий хорошо известен биологическим и социальным системам: какие бы громкие победы не одерживали карательно-исправительные органы, паразиты возрождались еще более совершенными, раскручивая новый виток борьбы «паразит — защита».

Думается, развитие компьютерной вирусологии пойдет по аналогичному пути, а событие, о котором я упоминал в начале статьи, только подтверждает это предположение.

САМАЯ «ПЕРСПЕКТИВНАЯ» ЗАЩИТА

Как уберечь машину от проникновения вирусов? Какой респиратор надеть? Какого сторожа приставить?

Проще всего установить на диск надежный детектор, способный находить вирусы по оставленным следам (обрывку кода). Правда, и такой «сыщик» надежно распознает ограниченное число вирусов, после чего начинает бросаться на подозрительные прикладные программы (аналог аллергии после большого числа прививок) или потребует слишком много времени на проверку. Впрочем, совершенствование вирусов исчерпает возможности таких детекторов очень и очень скоро.

Можно призвать другого «стража», узнающего вирусы по почерку. Именно на этот путь, предлагающий всяческие панацеи и абсолютные защиты, возлагают надежды многие программисты. Действительно, этот прием позволяет распознавать огромное число вирусов, но не искореняет зла, а лишь стимулирует создателей вирусов к поиску новых решений.

Ревизор, находящий вирусы по изменению содержимого зараженного файла или сектора на диске, — тоже не панацея. Общая проверка всех файлов требует времени. Иногда его можно сократить, используя внутрисистемную самопроверку или приставив штатного ревизора. Но в первом случае длина каждой программы увеличится, а во втором — снизится надежность контроля. Да и к любому разумному алгоритму можно подобрать ключ — способ заражения, не изменяющий контрольные параметры файла.

Все эти методы ориентируются на приметы «чужаков». Но если вирусов много и армия их стремительно пополняется, то гоняться за каждым «чужаком» в отдельности будет накладно. Гораздо проще создать эффективные процедуры распознавания «своих». Программы сами сообщают вам свои нестандартные контрольные параметры, а возможно, и процедуры их проверки, или поручат это операционной системе. Действи-

тельно, если ревизор побайтно подсчитывает контрольную сумму файла, то легко представить многоступенчатый вирус, который не изменит ни контрольную сумму (благодаря подбору байтов в своем буфере), ни длину файла. Если же каждая программа (или каждая операционная система) будет сама подсчитывать контрольные суммы, которые со временем могут меняться, то подделка станет затруднительной.

Не исключено, что программа при запуске будет сама сообщать о своих действиях, что позволит контролировать как присутствие «своих» и «чужих», так и отсутствие ошибок и сбоев. Это напоминает работу иммунной системы, которая не только реагирует на инородные белки, но и следит за постоянством генетического состава вообще.

Как известно, паспортная система не искоренила преступность, но заметно сократила ее экологическую нишу, породив попутно новые типы преступлений — подделку и кражу документов.

По аналогии можно предположить, что следующий виток борьбы «вирус — защита» будет раскручиваться вокруг контрольных параметров, удостоверяющих «личность» программы.

Кризис средств защиты, о котором так много говорили, пока не наступил. Сегодня защита намного сильнее нападения. А вот когда придется сменить столь модные детекторы на другие, не отработанные еще методы, — трудности появятся. Готовиться к этому нужно уже сегодня.

ЧТО НАС ЖДЕТ

Раньше, когда не было надежной защиты, вирусы поражали файлы и маскировались от оператора. Теперь же набирающая обороты индустрия защиты изменила приоритеты: для разработки самомаскирующихся вирусов или вирусов, поражающих кроме программных еще и объектные файлы, требуется гораздо больше времени, чем на разработку соответствующего детектора. Действительно, степень развития эпидемии определяется лишь временем создания эффективной защиты. Поэтому преимущество получают вирусы, максимально затрудняющие ее разработку.

Характерный пример подобного вируса — серия «Yankee Doodle». На коротком отрезке кода автор сумел разместить кроме веселой музыки защиту от трассировки, самовосстановление кода, подчинение ранних версий вируса более поздним. Но даже для столь изощренного «Yankee Doodle» разработать детекторы не сложнее, чем для других вирусов. Видимо самомодификация

кода и алгоритма станет необходимым атрибутом вирусов следующего поколения. Например, случайные вставки кода, не меняющие алгоритма вируса (прибавить ноль, отнять ноль), сделают невозможным надежное детектирование.

Простейшие самомодифицирующиеся вирусы уже появились. Пока их ловят без особого труда, но лиха беда — начало. Интересно, что механизм модифицирования (даже вопреки желанию авторов вирусов) уже существует: как правило, новый вирус, обогащенный изменениями и дополнениями «соавторов», появляется в нескольких вариантах. Пока их немного, но дело в другом — есть принципиально действующая модель. И если число модификаций увеличится до 100 тысяч, эффективное детектирование будет невозможно. А если новые вирусы станут появляться каждую минуту, не помогут никакие сети быстрого оповещения о вирусной опасности.

САБЛИ В НОЖНЫ

Движущая сила вирусологии — микросоревнование конкретных программистов (по разные стороны баррикад), подверженных субъективным пристрастиям и недолголюбивающих друг друга, а следовательно, не представляющее интереса для большинства.

От вирусологии, не учитывающей взаимодействия вирус — защита, может остаться одна голая классификация и несколько моральных заповедей. Поэтому обескураживают призывы ограничить публикации о вирусах. И если моральные устои вирусологии хорошо просматриваются, то неуважение к способностям авторов вирусов (молодой балбес, «юное дарование», ущербная личность...) просто наивно, так как уровень написания вирусов определяет уровень защиты.

Компьютерный вирус очень молод, а компьютерная вирусология еще моложе. Именно ее зачаточное состояние породило всевозможные научные спекуляции, равно как и полемический стиль, при помощи которого их критиковали. Гибельные последствия вирусного нашествия авторитеты считают чем-то средним между революцией и экологической катастрофой. Это щекочет воображение и служит trampлином для некоторых заслуженных программистов, бросающихся в бурную общественную деятельность. А ведь паразит — он и в компьютере всего лишь паразит, но никак не предвестник скорого конца света.

Старинную романтическую схему: поимка паразита — вечный бой, можно заменить на более современную: планирование — использование.

Многие явления в обществе, изначально считавшиеся вредными, впоследствии признавали прогрессивными. И дело не в том, что шайка разбойников может в будущем оказаться политической партией и наоборот, а в том огромном вреде, который может принести поверхностная и варварская оценка явления. Грустная история нашей Родины — хорошее тому подтверждение. В этом смысле уже не так забавно выглядят наши знатные программисты, ведущие яростную борьбу за чистоту компьютерных рядов.

Именно поэтому надо не запрещать создание вирусов (не путать с нанесением ущерба), загоняя их авторов в подполье, а наоборот, легализовать, устраивая конкурсы вирусных программ. Это соответствует не смотря «воровских отмычек», а форуму нового общественного движения. И тогда в открытом споре сойдутся атака и защита к огромной пользе для защиты, которая перестанет быть вечно опаздывающей.

Вот когда придется действительно думать, а не приписывать раз в неделю несколько новых масок в табличку и несколько новых строчек в файл README.

И если защита будет сооружаться с помощью самих авторов вирусов, то ее эффективность резко возрастет. Подпольные программисты обретут настоящую известность, к которой они так стремятся.

В. Г. ВЕСЕЛОВ

